**Instructions.** Answer each of the questions on your own paper, and be sure to show your work so that partial credit can be adequately assessed. There is a total of 70 points possible. Put your name on each page of your paper.

1. [**12 Points**] Let $m = 143$ and $n = 176$.

   (a) Calculate the greatest common divisor $d = \gcd(m, n)$.

   ▶ **Solution.** Use the Euclidean Algorithm:

$$\begin{aligned} 176 &= 1 \cdot 143 + 33 \\ 143 &= 4 \cdot 33 + 11 \\ 33 &= 3 \cdot 11. \end{aligned}$$

   Therefore, $d = \gcd(143, 176) = 11$. ◀

   (b) Write $d$ in the form $sm + tn$ for some integers $s$ and $t$.

   ▶ **Solution.** Reverse the above steps to get:

$$\begin{aligned} 11 &= 143 - 4 \cdot 33 \\ &= 143 - 4(176 - 1 \cdot 143) \\ &= 5 \cdot 143 - 4 \cdot 176. \end{aligned}$$

◀

2. [**12 Points**] Use induction to prove **one** of the following. Take your pick. (Just make a direct induction proof. Do not assume any other facts about congruences or summation formulas.)

   (a) For any positive integer $n$, $n^3 + 5n$ is a multiple of 3.

   ▶ **Solution.** Let $S(n)$ be the statement: $n^3 + 5n$ *is a multiple of* 3 *for the integer* $n$. We will use induction to show that $S(n)$ is true for all integers $n \geq 1$.
   ***Base Step.*** If $n = 1$ the statement $S(1)$ becomes: $1^3 + 5 \cdot 1$ *is a multiple of 3.* Since $1^3 + 5 \cdot 1 = 6$ it follows that $S(1)$ is a true statement.
   ***Inductive Step.*** For a given integer $n \geq 1$, assume that $S(n)$ is a true statement. Thus we are assuming that $n^3 + 5n$ is a multiple of 3 for the given integer $n$. That is, we are assuming that, for the given integer $n$, $n^3 + 5n = 3k$ for some integer $k$. Then

$$\begin{aligned} (n+1)^3 + 5(n+1) &= (n^3 + 3n^2 + 3n + 1) + (5n + 5) \\ &= (n^3 + 5n) + 3n^2 + 3n + 6 \\ &= 3k + 3(n^2 + n + 2) = 3(k + n^2 + n + 2). \end{aligned}$$

   Thus, we have shown that if $n^3 + 5n$ is a multiple of 3, then $(n+1)^3 + 5(n+1)$ is also a multiple of 3. Therefore, we have shown that if $S(n)$ is true, then so is $S(n+1)$.
   By the principle of mathematical induction, $S(n)$ is true for all natural numbers $n \geq 1$. ◀

   (b) For any positive integer $n$, $\sum_{k=1}^{n}(2k + 1) = n(n + 2)$.

▶ **Solution.** Let $S(n)$ be the statement

$$\sum_{k=1}^{n}(2k+1) = n(n+2)$$

for the integer $n$.

We will use induction to show that $S(n)$ is true for all integers $n \geq 1$.

***Base Step.*** If $n = 1$ the statement $S(1)$ becomes

$$2 \cdot 1 + 1 = 1(1+2),$$

which is a true statement, since both sides are equal to 3.

***Inductive Step.*** For a given integer $n \geq 1$, assume that $S(n)$ is a true statement. Thus we are assuming that

$$\sum_{k=1}^{n}(2k+1) = n(n+2)$$

for the given integer $n$. Then for $n+1$ we get

$$\begin{aligned}\sum_{k=1}^{n+1}(2k+1) &= \left(\sum_{k=1}^{n}(2k+1)\right) + 2(n+1) + 1 \\ &= n(n+2) + 2(n+1) + 1 \text{ (by the induction hypothesis } S(n)) \\ &= n^2 + 2n + 2n + 2 + 1 = n^2 + 4n + 3 = (n+1)((n+1)+2).\end{aligned}$$

Therefore, we have shown that if $S(n)$ is true, then so is $S(n+1)$.

By the principle of mathematical induction, $S(n)$ is true for all natural numbers $n \geq 1$. ◀

3. **[10 Points]** Use properties of congruences to compute the following. Express your answers as the least residue $\pmod{n}$, that is, in the form $x \pmod{n}$ where $0 \leq x < n$. Make the arithmetic as easy as possible.

   (a) $708 \cdot 75 \cdot 6999 \pmod{7}$

   ▶ **Solution.** $708 \equiv 1 \pmod{7}$, $75 \equiv 5 \pmod{7}$, and $6999 \equiv -1 \equiv 6 \pmod{7}$. Therefore,

   $$708 \cdot 75 \cdot 6999 \equiv 1 \cdot 5 \cdot 6 \equiv 30 \equiv 2 \pmod{7}.$$

   ◀

   (b) $7^5 + (602)^5 \pmod{6}$

   ▶ **Solution.** $7 \equiv 1 \pmod{6}$ and $602 \equiv 2 \pmod{6}$. Thus,

   $$7^5 + (602)^5 \equiv 1^5 + 2^3 \equiv 1 + 32 \equiv 33 \equiv 3 \pmod{6}.$$

   ◀

4. **[12 Points]** Short answer questions.

(a) Fill in the blanks to complete the statement of the division algorithm: Let $a$ and $b$ be integers with $b > 0$. Then there exist unique integers $q$ and $r$ such that $\boxed{a = bq + r}$ where $\boxed{0 \leq r < b}$.

(b) Euclid's Lemma states: Let $a$ and $b$ be integers and let $p$ be a $\boxed{\text{prime}}$ number.

If $p \mid ab$, then $\boxed{p \mid a \text{ or } p \mid b.}$.

(c) **T**rue or **F**alse. If, for nonzero integers $a$, $b$, $d$, there are integers $x$ and $y$ with $ax+by = d$, then $d$ is the greatest common divisor of $a$ and $b$. **False** Example: $3 \cdot 2 + 2 \cdot (-2) = 2$ but $\gcd(3, 2) = 1$.

(d) Define a binary operation $\circ$ on the integers $\mathbb{Z}$ to be ordinary subtraction. That is, $a \circ b = a - b$. Is 0 an identity element for the binary operation $\circ$? Explain. **Answer:** No, 0 is not an identity since $a \circ 0 = a - 0 = a$ but $0 \circ a = 0 - a = -a \neq a$ if $a \neq 0$.

5. **[12 Points]** Define a relation $\sim$ on $\mathbb{Z}_8$ by $x \sim y$ if $x^2 = y^2$, where $x, y \in \mathbb{Z}_8$.

(a) Verify that $\sim$ is an equivalence relation on $\mathbb{Z}_8$.

▶ **Solution.** To show that $\sim$ is an equivalence relation, it is necessary to show that it is (1) reflexive, (2) symmetric, and (3) transitive.

(1) If $x \in \mathbb{Z}_8$ then $x^2 = x^2$ so $x \sim x$, and $\sim$ is reflexive.

(2) If $x, y \in \mathbb{Z}_8$ and $x \sim y$ then $x^2 = y^2$. Since $=$ is symmetric, $y^2 = x^2$ so that $y \sim x$. Hence $\sim$ is symmetric.

(3) If $x, y, z \in \mathbb{Z}_8$ with $x \sim y$ and $y \sim z$, then $x^2 = y^2$ and $y^2 = z^2$. But $=$ is transitive, so $x^2 = z^2$ and hence $x \sim z$. Thus, $\sim$ is transitive.

Since $\sim$ is reflexive, symmetric, and transitive, it is an equivalence relation. ◀

(b) Find all of the distinct equivalence classes for the equivalence relation $\sim$.

▶ **Solution.** Consider the following table summarizing the calculation of $x^2$ for all $x \in \mathbb{Z}_8$:

| $x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| $x^2$ | 0 | 1 | 4 | 1 | 0 | 1 | 4 | 1 |

There is an equivalence class for each distinct value of $x^2$. Thus, the equivalence classes are

$$[10] = \{0, 4\}, \quad [1] = \{1, 3, 5, 7\}, \quad [2] = \{2, 6\}.$$

◀

6. **[12 Points]** Let $G_1 = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a, b, c \in \mathbb{R}, ac \neq 0 \right\}$ and $G_2 = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a, c \in \mathbb{R}, ac \neq 0, b \in \mathbb{Z} \right\}$.

(a) Show that $G_1$ is a subgroup of $\mathrm{GL}_2(\mathbb{R})$.

▶ **Solution.** Note that $G_1$ is just the set of all upper triangular $2 \times 2$ matrices with entries in $\mathbb{R}$. That is, $G_!$ is the set of invertible $2 \times 2$ matrices with real entries, such that the entry in the second row, first column is 0, and this is the only restriction on an invertible $2 \times 2$ matrix for being in $G_1$. Since $\det \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} = ac - b \cdot 0 = ac \neq 0$ it follows that $G_1$ is a subset of $\mathrm{GL}_2(\mathbb{R})$. To check that $G_1$ is a subgroup of $\mathrm{GL}_2(\mathbb{R})$, we need to check that the three conditions of Proposition 3.30 are satisfied.

(1) The identity of $\mathrm{GL}_2(\mathbb{R})$ is the identity matrix $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. This is in $G_1$ since the entry in the second row first column is 0, which is the only condition for being in $G_1$.

(2) Suppose $A$, $B \in G_1$. Then $A = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}$ and $B = \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix}$ so

$$AB = \begin{bmatrix} a_1a_2 & a_1b_2 + b_1ac_2 \\ 0 & c_1c_2 \end{bmatrix}.$$

Since $AB$ is upper triangular, $AB \in G_1$ and $G_1$ is closed under multiplication.

(3) If $A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in G_1$, then the inverse of $A$ in $\mathrm{GL}_2(\mathbb{R})$ is

$$A^{-1} = \frac{1}{ac}\begin{bmatrix} c & -b \\ -0 & a \end{bmatrix} = \begin{bmatrix} 1/a & -b/(ac) \\ 0 & 1/c \end{bmatrix}$$

which is upper triangular and hence $A^{-1} \in G_1$. ◀

(b) Show that $G_2$ is not a subgroup of $\mathrm{GL}_2(\mathbb{R})$.

▶ **Solution.** To show that $G_2$ is not a subgroup of $\mathrm{GL}_2(\mathbb{R})$ (even though it is a subset of $G_1$ and hence a subset of $\mathrm{GL}_2(\mathbb{R})$) it is sufficient to show that one of the above 3 conditions for being a subgroup fails. Let $A = \begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix}$. Then $A \in G_2$ but $A^{-1} = \begin{bmatrix} 1/2 & -1/2 \\ 0 & 1 \end{bmatrix}$ and this is not in $G_2$ since the upper right entry is not an integer. Thus, $G_2$ is not closed under inverses and hence is not a subgroup. ◀

**Bonus (10 Points)** If $G$ is a group with $x^2 = e$ for all $x \in G$, where $e$ is the identity, prove that $G$ is abelian.

▶ **Solution.** The condition that $x^2 = e$ means that $x = x^{-1}$ for all elements $x \in G$. Then, if $a$, $b \in G$, then

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba$$

where the second equality is Proposition 3.19. Since $a$ and $b$ are arbitrary, it follows that $ab = ba$ for all $a$, $b \in G$ and hence $G$ is abelian. ◀